

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A CRIMINAL COMPLAINT
AND ARREST WARRANT

I, James V. Richardson, a Special Agent (SA) with Homeland Security Investigations,
being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (“HSI”) since 2009, and am currently assigned to the office of the Resident Agent in Charge (RAC), Providence, RI. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center in Brunswick, GA, and as a member of the Rhode Island Internet Crimes Against Children (ICAC) Task Force conducting these types of investigations. I have investigated child pornography cases and related sexual offenses on a full time basis since approximately January 2010. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have conducted and assisted in conducting numerous investigations into the violation of both state and federal laws relating to the possession, receipt, transportation, distribution, and production of child pornography and obscene visual representations of the sexual abuse of children over the Internet. I have reviewed hundreds of images and videos of actual and suspected child pornography, child erotica, and obscene visual representations of the sexual abuse of children. Moreover, I am a federal law enforcement officer who is engaged in

enforcing the criminal laws, including but not limited to, violations of 18 U.S.C. §§ 1470, 2252, and 2252A, 2422, and 2423.

2. This affidavit is submitted in support of an application for a criminal complaint charging Herbert J. RODAS, (D.O.B. xx/xx/1996) ("RODAS") with transferring obscene material to a minor in violation of 18 U.S.C. § 1470; enticement of a minor to engage in illicit sexual activity in violation of 18 U.S.C. § 2422(b); and travelling in interstate or foreign commerce with the intent to engage in illicit sexual activity in violation of 18 U.S.C. § 2423(b).

3. On July 10, 2019, I applied for a search warrant to search the premises located at 136 Chandler Avenue, Pawtucket, RI 02860 and electronic media storage devices and the person of RODAS and submitted an affidavit in support. That affidavit is attached to this affidavit as Exhibit A and incorporated by reference and restated herein for purposes of this affidavit.

4. On July 11, 2019, the search warrant was executed by myself, other members of HSI, and the Rhode Island Internet Crimes Against Children (ICAC) task force. The residence was occupied by RODAS and his mother.

5. During the execution of the search warrant, RODAS was interviewed by myself and RISP Detective Brian Macera at the residence. RODAS was advised that he was not under arrest and also advised of his Miranda rights. RODAS signed the advice of rights form and agreed to voluntarily speak with us. RODAS then proceeded to state, among other things the following:

- RODAS admitted to engaging in online chats with the individual described as Minor Victim 1 ("MV1") in Exhibit A.
- RODAS admitted that he met MV1 on the social media application "Omegle" and that subsequently most of their conversations took place as image exchanges and typed

communications on “Snapchat” a social media application where images, videos and text chats can be exchanged, and video chats “FaceTime,” an application on Apple iPhone devices that allows video phone calls.

- RODAS admitted that during these online conversations, approximately one week into conversing with MV1 he believed her age to be 14. He believed he turned the conversation sexual in nature. He admitted sending images of his penis to MV1 via Snapchat and livestreaming himself masturbating via FaceTime.
- RODAS admitted requesting specific naked pictures of MV1. He specifically requested pictures of MV1’s breasts, and also requested pictures of MV1’s vagina. RODAS further admitted that MV1 complied with his request and sent the images.
- RODAS admitted that he knew MV1 was a minor; RODAS said he thought she was 14 years old. I asked RODAS if he recalled that MV1 initially told him she was 15 years old and later stated she was actually 13 years old. RODAS replied words to the effect of, “Yeah, something like that.”
- RODAS admitted travelling from Rhode Island to Canada to meet with MV1 in April 2019. RODAS told his parents he had a work trip to Canada. RODAS got a ride to Logan Airport in Boston from his father. RODAS flew from Logan Airport to a final destination of Winnipeg, Manitoba, Canada. He did not remember the connecting airport.
- RODAS admitted that he arrived in Canada on a Thursday¹ in April, and met MV1 twice that day; the first time he met her while she was walking her dog; he met her again later that night. RODAS claimed MV1 snuck out of her house to meet him down the

¹ April 25, 2019 was a Thursday.

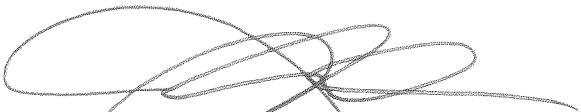
street. RODAS picked her up in his rental car. RODAS stated that MV1 performed oral sex on him in the car. RODAS stated they then had sexual intercourse in the car. RODAS stated that he used a condom but he did not ejaculate into the condom.

Rather, he removed the condom and masturbated in front of MV1. RODAS stated that he noticed blood from MV1's vagina.

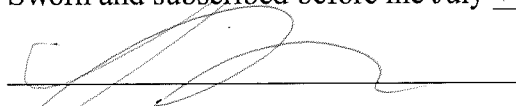
- RODAS admitted that over the course of the next two days, RODAS admitted to having sexual intercourse with MV1 an additional two times in his hotel room.
- RODAS admitted that upon returning to Rhode Island, he sent MV1 messages threatening to disclose their relationship to her mother and boyfriend. Initially, RODAS claimed this was simply "roleplaying." RODAS subsequently admitted it was not roleplaying.

6. During the execution of the search warrant, RODAS' passport, a boarding pass from Toronto Canada to Boston for RODAS' return trip from Canada, and Super 8 Motel receipt were located.

7. Based on the above, I believe there is probable cause to arrest Herbert J. RODAS for transferring obscene material to a minor in violation of 18 U.S.C. § 1470; enticement of a minor to engage in illicit sexual activity in violation of 18 U.S.C. § 2422(b); and travelling in interstate or foreign commerce with the intent to engage in illicit sexual activity in violation of 18 U.S.C. § 2423(b).


James V. Richardson
Special Agent
Homeland Security Investigations

Sworn and subscribed before me July 11 2019.



HON. LINCOLN D. ALMOND
UNITED STATES MAGISTRATE JUDGE

EXHIBIT A

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, James V. Richardson, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with United States Department of Homeland Security (DHS), Immigrations and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and am assigned to the office of the Resident Agent in Charge, Providence, RI. I have been an agent of HSI since 2009. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, and the transfer of obscene material to minors, including but not limited to, violations of 18 U.S.C. §§ 1470, 2252, and 2252A, 2422, and 2423. I have received training in the investigation of child pornography, child exploitation, and transportation of minors, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).

2. I am currently participating in an investigation relating to violations of federal law by Herbert J. RODAS for transferring obscene material to a minor in violation of 18 U.S.C. § 1470; possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(4)(B); receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2); enticement of a minor to engage in illicit sexual activity in violation of 18 U.S.C. § 2422(b); and travelling in interstate or foreign commerce with the intent to engage in illicit sexual activity in violation of 18 U.S.C. § 2423(b).

3. I submit this affidavit in support of an application to search the person of Herbert J. RODAS (hereinafter "RODAS") and RODAS' residence, the premises located at [REDACTED] Pawtucket, RI 02860 (the "SUBJECT PREMISES"), and the content of any

electronic media storage devices or media located therein, as more fully described in Attachment A, which is incorporated herein by reference; and to seize evidence, instrumentalities, fruits of crime, and contraband as more fully described in Attachment B, which is also incorporated herein by reference.

4. The statements in this affidavit are based in part on information provided by other law enforcement agencies to include the Rhode Island State Police (RISP) and the Winnipeg, (Canada) Police Service (WPS).

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

5. In June 2019, the Winnipeg Police Service (WPS) contacted the Rhode Island State Police (RISP) Internet Crimes Against Children (ICAC) Task Force and Homeland Security Investigations (HSI) Providence, RI to report the sexual assault of a 13-year-old female. According to the information received from WPS, Herbert J. RODAS travelled from the United States to Canada to engage in sexual activity with the minor victim (hereinafter "MV1").

6. In January 2019, RODAS and MV1 met on a chat website and began communicating. Initially, MV1 identified herself as a 15-year-old female and RODAS identified himself as a 23-year-old male. Within 10 to 15 minutes of the initial communication, the talk turned sexual with RODAS telling MV1 about sexual things he was into and asking MV1 to touch herself. After several requests from RODAS, MV1 did masturbate for RODAS.

7. In approximately February 2019, MV1 told RODAS that she was actually 13-years-old and RODAS revealed that he was actually 22-years-old. RODAS continued to communicate with MV1, a through a variety of facilities of interstate and foreign commerce, including Omegle, Facebook, Instagram and Snapchat through April 2019. At RODAS' request, on multiple occasions MV1 sent RODAS images of herself in various stages of undress, to include fully nude photos. RODAS also sent MV1 images of his erect penis and at times,

masturbation and ejaculation images. RODAS communicated to MV1 that he wanted to marry her and that he wished that she was 18-years-old so that she could run away with him. It should also be noted that when communicating via Snapchat, a user's location is often listed and RODAS' location was often listed as [REDACTED] Pawtucket, RI.

8. On April 25, 2019, RODAS flew from United States to Canada via Air Canada. RODAS reserved a room at a Super 8 motel and paid with cash. RODAS used his full name, credit card and the email address [REDACTED]@hotmail.com for the reservation. Over the next three days, RODAS met with MV1 four times and had sexual intercourse with MV1 using a condom on three of those occasions. MV1 kept the condom from their first sexual encounter and turned it over to the WPS. WPS is having the condom tested for DNA and the results are pending. RODAS and MV1 took photos while they were together in Canada. WPS sent those images to HSI Providence and I reviewed the images. One image is of RODAS and MV1 in a car believed to be the car rented by RODAS. Both RODAS' and MV1's faces can be seen in this image. I compared the image to another known image of RODAS and positively identified him. The other image is of RODAS and MV1 holding hands, also in a car.

9. Once RODAS returned to the United States, he tried to continue communicating with MV1 via facilities of interstate and foreign commerce, but MV1 wasn't communicating back. RODAS then began threatening MV1 through these communications by saying that he would reveal their relationship to her boyfriend and her mother. RODAS also threatened to report the incident himself to the local police. In two of the communications, RODAS says "I regret what I did. I'm sorry. Please respond with it. Please!" and "Forgive me for what I have done."

10. A check of a U.S. Customs and Border Patrol database revealed that RODAS did fly from Boston, MA to Canada on April 25, 2019, returning to Boston, MA on April 28, 2019.

RODAS used the email address [REDACTED]@yahoo.com for these reservations. RODAS also used the phone number 401-[REDACTED]

11. I conducted a query of a commercial database for Herbie J. RODAS, date of birth [REDACTED] 1996. The results revealed that RODAS is currently living at [REDACTED] Pawtucket, RI 02860. The results also revealed that phone number 401-[REDACTED] is associated with RODAS. Accordingly, I believe that RODAS traveled from Rhode Island to Canada through Boston, MA on April 25, 2019.

12. I conducted a query of a publicly available database for the address [REDACTED] Pawtucket, RI 02860. The results revealed that the property is a white, one and a quarter story bungalow style home owned by [REDACTED] Rodas since 2005.

13. On July 8, 2019, I sent a request to the Rhode Island Fusion Center for RI driver's license information for RODAS. The RI Fusion Center returned the following information:

Name: Herbert J. RODAS
Address: [REDACTED] Pawtucket, RI 02860
SSN: [REDACTED] 5465
DOB: [REDACTED] 1996
RIDL: [REDACTED]

14. On July 9, 2019, I conducted surveillance at [REDACTED] Pawtucket, RI 02860. The residence is described as a white one family residence with red shutters and the number "136" to the trim above the front porch.

**CHARACTERISTICS COMMON TO PERSONS WHO ENGAGE IN
CHILD SEXUAL EXPLOITATION**

15. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have collaborated, I have learned that there are certain characteristics that are generally common to offenders who access, send, distribute, exhibit, possess, display, transport, manufacture, or produce material which depicts minors engaged in sexually explicit conduct, or who engage in sexually explicit communications with minors. Said material includes, but is not limited to, photographs and videos stored electronically on computers, digital devices, or related digital storage media.

16. Such offenders may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have that stem from viewing children engaged in sexual activity or in sexually suggestive poses, whether in person, in photographs or other visual media, or from literature describing such activity.

17. Such offenders may collect sexually explicit or suggestive materials in a variety of media, including digital photographs, videos, or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to facilitate contact offenses – that is, to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

18. Such offenders almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or

images of children typically retain their cache for many years. In my training and experience, I am aware that such offenders often

19. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a, "SD card," computer or surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the offender's residence, inside the offender's vehicle, or, at times, on his person, to enable the individual to view the child pornography images, which are highly valued.¹

20. Some of these individuals, however, have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis, presumably to avoid criminal liability. Importantly, as described in more detail below, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.²

21. Such offenders also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists or other record of individuals with whom they have been in contact and who share the same interests in child pornography.

¹ See *United States v. Morales-Aldahondo*, 524 F.3d 115, 117-119 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections);

² See *United States v. Seiver*, 692 F.3d 774, 775-776 (7th Cir. 2012) (in context of staleness challenge, collecting and agreeing with cases from the 4th, 5th, 6th, and 9th Circuits that acknowledge the ability of forensic examiners to recover evidence of child pornography even after such files are deleted by a user).

22. Such offenders prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if such an offender uses a portable device (such as a mobile phone or gaming device) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home -- here, the SUBJECT PREMISES, as set forth in Attachment A.

23. Based upon the foregoing, I believe that Herbert J. RODAS likely displays characteristics common to individuals who access with the intent to view and possess, collect, receive, or distribute child pornography. He exchanged sexually explicit images with an individual he knew to be a minor over a period of months, travelled internationally in order to have sex with her, and attempted to continue the relationship upon his return to the United States. I think it likely that RODAS continues to possess images of MV1, to include nude images which likely constitute child pornography under federal law. I also think it likely that RODAS continues to possess the sexually explicit images of his penis and masturbation/ejaculation images described above.

24. As such, I submit that there is probable cause to believe that contraband material depicting minors engaged in sexually explicit conduct and other evidence, instrumentalities, and fruits of violations of possession and access with intent to view child pornography 18 U.S.C. §§ 2252(a)(4) exist at the SUBJECT PREMISES, in addition to evidence of transfer of obscene material to a minor in violation of 18 U.S.C. § 1470, attempted enticement of a minor in violation of 18 U.S.C. § 2422(b), and travel in interstate and foreign commerce with the intent to engage in illicit sexual activity in violation of 18 U.S.C. § 2423(b).

SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND DATA

25. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even

years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from an old computer to a new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is usually required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

26. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software, or storage media, to ensure the accuracy and completeness

of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, computer-related documentation, and storage media ("computer equipment") be seized and subsequently processed by a qualified computer specialist in a laboratory setting, rather than in the location where it is seized. This is true because of:

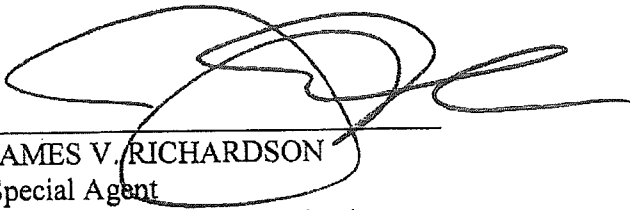
a. The volume of evidence: Storage media such as hard disks, SD cards, flash drives, CD-ROMs, and DVD-ROMs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine what particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements: Analyzing computer hardware, computer software, or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, password-protected, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

CONCLUSION

27. Based on the foregoing, I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1470, 2252(a)(2); 2252(a)(4)(B); 2422(b) and 2423(b), as described in Attachment B, are located at the SUBJECT PREMISES, as more fully described in Attachment A.

Sworn to under the pains and penalties of perjury,



JAMES V. RICHARDSON
Special Agent
Homeland Security Investigations

SUBSCRIBED and SWORN to before me on July 10, 2019.



HONORABLE LINCOLN D. ALMOND
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The premises to be searched include:

- A. The person of Herbert J. RODAS, a Hispanic male, standing 5'09", born in 1996.
- B. The content of any electronic media storage devices, including smart phones, or media located on the person of Herbert J. RODAS or found in the premises of [REDACTED] [REDACTED] Pawtucket, RI 02860.
- C. Premises located at [REDACTED] Pawtucket, RI 02860, more particularly described as a white one and a quarter-story house. The number "136" is clearly affixed to the trim above the front porch. The exterior of the premises is pictured below:



ATTACHMENT B
DESCRIPTION OF INFORMATION TO BE SEIZED

- I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. § 1470; 18 U.S.C. § 2252(a)(2); 18 U.S.C. § 2252(a)(4)(B); 18 U.S.C. § 2422(b) and 18 U.S.C. § 2423(b), including:
- A. Records and tangible objects pertaining to the following topics:
1. Child pornography and child erotica;
 2. Obscene materials;
 3. Communications with minors or others having access to minors that relate to the persuasion, inducement, enticement or coercion of a minor to engage in sexual activity for which any person could be charged with a criminal offense, or the transfer of obscene materials to a minor.
 4. Travel documents to include; passport; airline tickets; receipts; boarding passes; hotel receipts; rental car documents; souvenirs or other indicia of travel to Canada in April 2019.
 5. Photographic or digital media indicating a trip to Canada in April 2019,
- B. For any electronic media storage device, smart phone, computer hardware, including gaming devices such as Xbox or PlayStation, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):
1. evidence of who used, owned, or controlled the computer equipment;
 2. evidence of computer software that would allow others to control the items, evidence of the lack of such malicious software, and evidence of the

presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;
4. evidence of counter forensic programs and associated data that are designed to eliminate data;
5. evidence of the times the computer equipment was used;
6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;
7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media; and
8. evidence indicating the computer user's state of mind as it relates to the crime under investigation.

C. Records and tangible objects relating to the ownership, occupancy, or use of the SUBJECT PREMISES (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers); and

D. records, information, and items relating to the ownership or use of computer equipment and other electronic storage devices found in or on the SUBJECT PREMISES, including sales receipts, bills for Internet access, and handwritten notes.

II. All computer hardware, computer software, computer-related documentation, and storage media. Off-site searching of these items shall be limited to searching for the items described in Paragraph I.

DEFINITIONS

For the purpose of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, gaming device, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- D. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

H. "Obscene material" is any image or video representation containing material which the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; depicts in a patently offensive way, sexual conduct and taken as a whole, lacks serious literary, artistic, political, or scientific value such as patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated, patently offensive representation or descriptions of masturbation, excretory functions, and lewd exhibition of the genitals.